

### REMARKS

Assignee appreciates the detailed examination of the present application as evidenced by the Final Office Action mailed February 17, 2010 (hereinafter "Final Action"). In response, Assignee has amended independent Claims 1, 10, and 18 to clarify that the status information comprises both job category and authorized access zone information, which is not disclosed or suggested in the cited references. Accordingly, Assignee submits that all pending claims are in condition for allowance. Favorable reconsideration of all pending claims is respectfully requested for at least the reasons discussed hereafter.

#### **Independent Claims 1, 10, and 18 are Patentable**

Independent Claims 1, 10, and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent Publication No. US 2003/0023722 to Vinberg (hereinafter "Vinberg") in view of U. S. Patent Publication No. 2004/0148526 to Sands et al. (hereinafter "Sands"). Independent Claim 1 is directed to a method of outputting an alert and recites, in part:

...  
obtaining a status from a sensor;  
retrieving personnel information comprising identity and status  
information for the personnel from a database, the personnel information relating  
to the sensor;  
generating the alert;  
applying a filter to determine whether to modify a severity of the alert; and  
outputting the alert;  
wherein the status information comprises job category and authorized  
access zone information. (Emphasis added)

Independent Claims 10 and 18 include similar recitations. Thus, according to independent Claim 1 as amended, the personnel information stored in the database includes both identity and status information for the personnel. Moreover, the status information comprises both job category and authorized access zone information. Such embodiments are described, for example, on page 8, paragraph 24 of the Specification where the text explains that the personnel information can

include various identity information along with status information, such as job category and/or authorized access zones for the various individuals.

The Final Action acknowledges that Vinberg does not disclose retrieving personnel information comprising identity and status information from a database, but alleges that Sands provides the missing teachings. (Final Action, page 3). Sands is directed to a security method and system for authenticating a person's identity based on biometric information. (*See, e.g.*, Sands Abstract and paragraphs 7, 19, 24, and 37). The Final Action alleges that Sands discloses retrieving identity (biometric profile) and status information (disabled/not-disabled) information from a database. (Final Action, page 3). With respect to the status information comprising job category information, the Final Action alleges that Sands discloses this recitation in the table beneath paragraph 95 with "Admin" being a job category. (Final Action, page 4). The table beneath paragraph 95 of Sands provides a list of policies and respective descriptions of the biometric authentication requirements associated with those policies. As set forth in Sands' table, to be granted administrator access, one needs to request to login as an administrator and obtain two fingerprints from any two active users in the an administrator group. Sands does not provide any description of including an administrator designation (or other job category designation) for personnel in the storage medium 205 as recited in the independent claims. Rather, Sands explains in paragraph 50 that the storage medium is used to store biometric profiles that are associated with the various users either by name or some other user identification.

In response to this analysis, the Final Action alleges that Sands discloses the idea that users can be organized in a group, such as a group of individuals with administrator authority. The Final Action further alleges that such a group classification qualifies as job category information and, therefore, indirectly discloses retrieving job category status information from a database that includes both job category status information and authorized zone information. (Final Action, page 12). As stated above, however, Sands does not include any description of the storage medium as containing a database with both job category status information and

authorized zone information. Instead, Sands describes the storage medium 205 as containing biometric profiles. While Sands does disclose the concept of associating users in a group, there does not appear to be any disclosure of how this is done and no suggestion of doing so by storing the information in a database along with authorized zone information.

With respect to the status information comprising authorized access zone information, the Final Action alleges that Sands discloses this recitation in paragraph 73 and in block 415 of FIG. 4. (Final Action, page 4). Block 415 of FIG. 4 relates to the server software 120 retrieving configuration information for a location from which authentication is sought. Sands explains that this information "might comprise the type of scanners (fingerprint, eye, palm... etc) as well as the brand and biometric format that each device produces." (Sands, paragraph 71). Thus, block 415 of FIG. 4 does not describe specifying authorized access zones for personnel and storing such information in a database as recited in the pending independent claims. Turning next to paragraph 73 of Sands, this paragraph explains that certain locations may be disabled regardless of who is logging in. Assignee submits that Sands' description of the ability to disable certain locations from access does not anticipate specifying authorized access zones for personnel and storing such information in a database as recited in the independent claims. Accordingly, Assignee submits that Sands fails to disclose or suggest, at least, the teachings missing from Vinberg related to the status information retrieved from the database comprising job category and authorized access zone information.

In response to this analysis, the Final Action continues to allege that selectively enabling and disabling user login locations corresponds to authorized access zone information and also that paragraph 36 of Sands discloses the idea of defining the authentication requirements at each login location in the computer network. (Final Action, page 13). It appears that paragraph 36 of Sands refers to the idea of defining how a user is authenticated at each location in the network based on what type of biometric devices are located at each location. (Sands, paragraphs 35 and 36). The description in paragraphs 35 and 36 of Sands does not appear to disclose storing

authorized access zone information in the same database as job category information. Moreover, while Assignee does not agree that enabled/disabled login location information corresponds to authorized access zone information, even, for the sake of argument, if it were considered to correspond to authorized access zone information Sands does not disclose or suggest storing such information in the same database as job category information.

For at least the foregoing reasons, Assignee respectfully submits that independent Claims 1, 10, and 18 are patentable over Vinberg and Sands, and that Claims 2 - 9, 11 - 17, 19, and 20 are patentable at least per the patentability of independent Claims 1, 10, and 18.

#### **Dependent Claims Are Patentable**

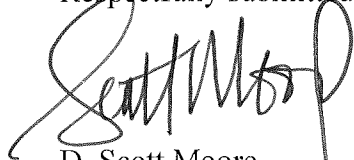
As each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Assignee does not believe that it is necessary to argue the allowability of each dependent claim individually. Assignee does not necessarily concur with the interpretation of these claims, or with the bases for rejection set forth in the Final Action. Assignee therefore reserves the right to address the patentability of these claims individually as necessary in the future.

#### **CONCLUSION**

In light of the above amendments and remarks, Assignee respectfully submits that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

In re: Jeffrey A. Aaron et al.  
Serial No.: 10/675,517  
Filed: September 30, 2003  
Page 10

Respectfully submitted,

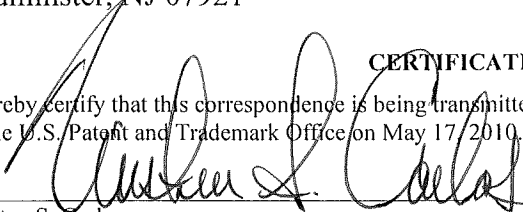


D. Scott Moore  
Registration No. 42,011

**USPTO Customer No. 39072**  
AT&T Legal Department – MB  
Attn: Patent Docketing  
Room 2A-207  
One AT&T Way  
Bedminster, NJ 07921

**CERTIFICATION OF TRANSMISSION**

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4) to the U.S. Patent and Trademark Office on May 17, 2010.



Kirsten S. Carlos